SSL-VPN機器に関する調査

インターネットVPN-WG
セコムトラストネット　若林　進二郎

2004 年 5月 18日

活動目的

- インターネットVPNを導入する際の注意点、安全なVPNを実現するための運用方法を分かり易く解説することで、インターネットVPNを普及させることを目指す。

活動内容

- 基本的には実機を使用した検証を通じて、構築・運用時の注意点を明らかにしてきた。
  - 2000年
    - 第1回 IPsec機器相互接続試験を実施
  - 2001年
    - 第2回 IPsec機器相互接続試験を実施
  - 2002年
    - 公衆無線LANを使用した、モバイルVPNに関する調査
  - 2003年
    - SSL-VPN機器に関する調査

SSL-VPN検証の背景

- 02年後半からSSL-VPNが注目されていた。
- 各社各様の製品仕様で、カタログだけではSSL-VPNの実力が分からなかった。
- SSL-VPNもWEBアプリとしてみたとき、脆弱性の問題が気になった。

脆弱性に関して

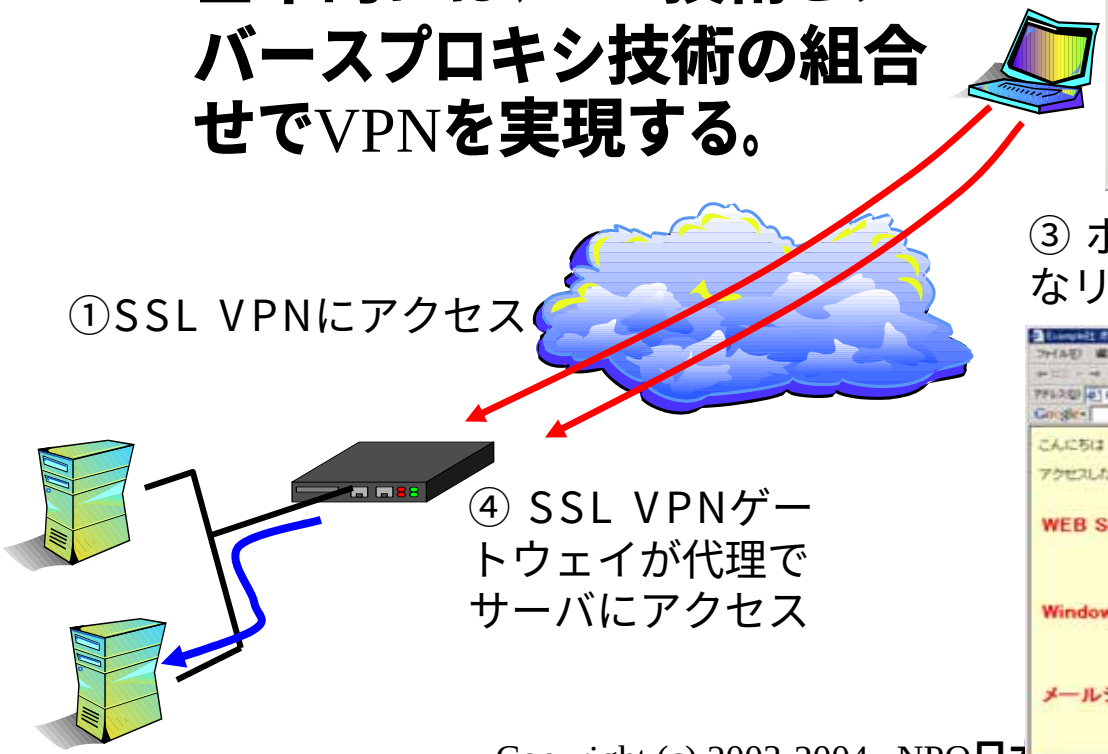
- ツールを使用して調査(KaVaDo社 ScanDo使用)
  - ツールでは脆弱性が発見されなかった。
- ライブラリの脆弱性
  - 多くの機器がOpenSSLやApacheを使用しているにも関わらず、これらに脆弱性が発見された時、メーカから情報が公開されない。

複雑な接続方式

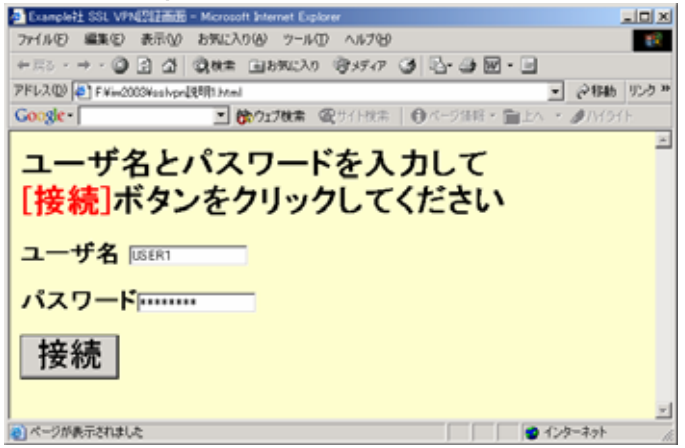
- クライアントレスと言いつつも
  - 非SSL アプリケーションなどを使用したい場合には、幾つかの接続方式がある。
  - リバースプロキシー方式
    - WEBブラウザだけを使用してアクセスする
    - 多くの製品は、WEBとWindowsファイル共有が使用可能
  - ポートフォワード方式
    - Javaアプレットをダウンロードし、社内リソースへの通信をSSL化して転送する。
    - TCP固定ポートのアプリケーションが使用可能
  - SSLトンネル方式
    - 専用クライアントを使用して、社内リソースへの通信をSSL化して転送する。
    - TCP/UDP問わずほとんどのアプリケーション使用可能

リバースプロキシー方式

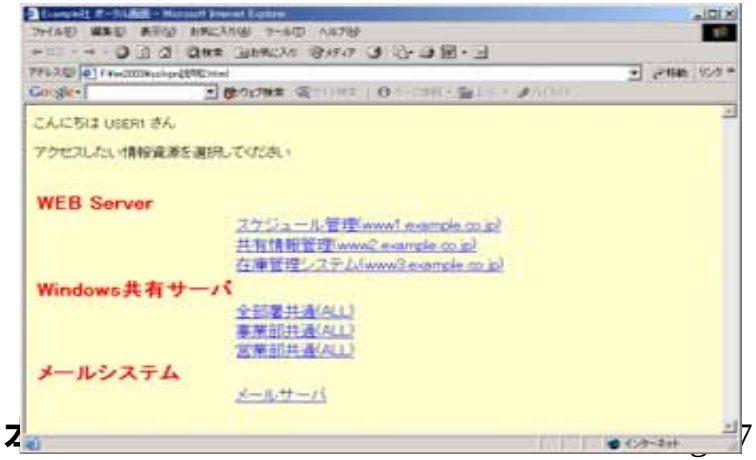
- SSL VPNとは？
  - SSLを利用してVPNを実現する技術
  - 基本的には、SSL技術とリバースプロキシ技術の組合せでVPNを実現する。



② 認証画面が表示され
認証情報を入力



③ ポータル表示されたアクセス可能なリソースから任意のリソースを選択



ポートフォワード方式

① ポータルから非SSL対応アプリを選択。

② Javaアプレットを自動的にダウンロードし起動する。

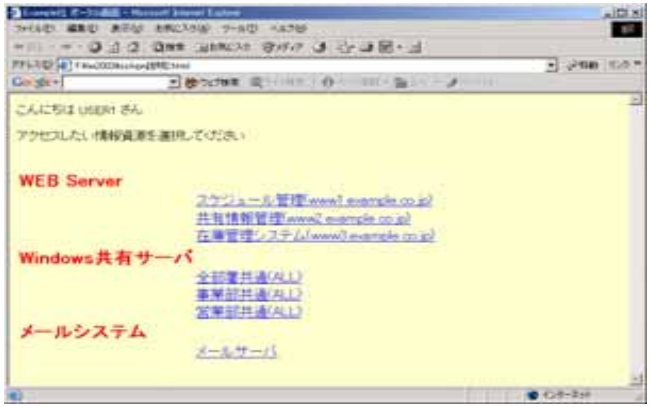
③ Javaはポートフォワード機能と、選択されたサーバのアドレスをhostsファイルに追加する。

④ 選択したリソースへのアクセスを開始すると、hostsファイル参照により、クライアント自身（Javaが受取る）宛に通信を行う。

④ 社内リソース宛の通信を受信したJavaは通信をSSL化してSSL VPNゲートウェイに転送

SSLトンネル方式

① ポータルから非SSL対応アプリを選択。



② 初めての場合はActiveXで自動的にクライアントアプリケーションをインストール

③ クライアントアプリケーションにより仮想インターフェースが設定される。

④ 選択したリソースへのアクセスを開始すると、その通信は仮想ドライバがSSL化しSSL VPNゲートウェイに転送する。

SSLトンネル時のパケットの構成

SSL-VPN導入時の注意点①

- **社内に居る時と、社外に居るときで操作が変わる。**
  - **すべてのリソースをポータル経由でアクセス**
    - **メール本文記述のURLや、クライアントPCのブックマークを使用して直接リソースにアクセスできない。**
- **クライアントアプリケーション**
  - **クライアントアプリケーションがインストールされる際には、Administrator権限が必要となる**
- **証明書の検証**
  - **クライアント証明書の検証が行われない製品が多い**
    - **SSLの標準では証明書の検証が行われないため、SSL VPNゲートウェイの実装も証明書の失効検証が行われない製品が多い。**
- **アクセス制御について**
  - **アクセス制御の設定変更が有効になるタイミングが製品によって異なる。**
    - **製品によっては、アクセス制御の設定変更時に全てのセッションが切断されることがある。**

SSL-VPN導入時の注意点②

- **パーシステンス関係**
  - 履歴ファイル、一時ファイル、キャッシュ、cookie、電子メールファイルの添付ファイルやダウンロードデータ等が利用したキオスク端末などに残ってしまう可能性がある
- **ユーザ認証**
  - 接続に際しての障壁が少ない反面、ID／パスワードでの認証では不正アクセスについての不安が残る
- **ログ管理**
  - 今回確認した機器については、ログ管理面についてあまり満足出来ない部分があった
    - ユーザ認証の成功／失敗レベルでしかログを残さない（一部製品）
    - ログの個別保存や検索機能がない

IPsec vs SSL-VPN

	IPsec	SSL-VPN
対応端末	OS依存	SSL対応WEBブラウザが稼動すればプラットフォームに依存しない。携帯電話やPDAもOK
対応アプリケーション	IP上で稼動するアプリケーション	製品依存
使い勝手	リソースへのアクセスはローカル環境と同様のオペレーションで可能	リソースへのアクセスはポータル経由
ネットワーク環境依存	NAT-Tや、IPsec-DHCPでほぼ解決しているが、MTU問題が若干残る	NATや名前解決の問題は発生しない。
アクセス制御	IPアドレス単位で実施	リソース単位で実施 (例えばURL単位やフォルダ単位)
費用	小規模の場合、SSL VPNより割安 大規模の場合、SSL VPNより割高になる可能性が高い	小規模の場合、IPsec VPNより割高 大規模の場合、IPsec VPNより割安になる可能性が高い

現状では、使用したい端末とアプリケーションとのバランスを考慮してVPN技術を選択することが、失敗しないリモートアクセスVPNに繋がる